(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
7 février 2002 (07.02.2002)

PCT

(10) Numéro de publication internationale
WO 02/11399 A1

(51) Classification internationale des brevets[7] : H04L 29/06

(21) Numéro de la demande internationale :
PCT/FR01/02466

(22) Date de dépôt international : 27 juillet 2001 (27.07.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00/09874 27 juillet 2000 (27.07.2000) FR

(71) Déposants et
(72) Inventeurs : **PETIT, Philippe** [FR/FR]; 1, rue Jules Ferry, F-95880 Enghien les Bains (FR). **AUGUSTIN, Alexandre** [FR/FR]; 9, rue des Merles, F-94440 Villecresnes (FR).

(74) Représentant commun : **PETIT, Philippe**; 1, rue Jules Ferry, F-95880 Enghien les Bains (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *avec rapport de recherche internationale*
— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) **Title:** DEVICE FOR PROTECTING COMPUTER SYSTEMS AGAINST INTRUSIONS AND ABUSES DERIVED FROM OPEN COMMUNICATION NETWORKS

(54) **Titre :** DISPOSITIF DE PROTECTION DES SYSTEMES INFORMATIQUES CONTRE LES INTRUSIONS OU MALVEILLANCES ISSUES DES RESEAUX DE COMMUNICATION OUVERT SUR L'EXTERIEUR

(57) **Abstract:** The invention concerns a device for securely browsing or using message services on external communication networks, such as Internet. It consists of a box containing a system for dialogue on said external networks and a communication system with work console completely isolating the internal network of the enterprise, the organisation or the structure from said insecure external structures. The device is particularly designed for structures wishing to provide fail-safe protection for their computer system and their private networks against intrusions and abuses possibly caused by external communication networks.

(57) **Abrégé :** L'invention concerne un dispositif permettant de naviguer ou d'utiliser des messageries sans risque sur des réseaux de communication externe de type "internet". Il est constitué d'un boîtier contenant un système permettant le dialogue sur ces réseaux externes et un système de commutation de console de travail isolant complètement le réseau interne de l'entreprise, de l'organisme ou de la structure des dits réseaux externes à risques. Le dispositif est particulièrement destiné aux structures désirant protéger, sans aucune faille, leur informatique et leur réseau privé des intrusions et malveillances éventuellement occasionnées par l'usage des réseaux externes de communication.

WO 02/11399 A1

Dispositif de protection des systèmes informatiques contre les intrusions ou malveillances issues des réseaux de communication ouvert sur l'extérieur.

La présente invention concerne un dispositif pour protéger les systèmes informatiques contre les intrusions ou malveillances issues d'un réseau de communication ouvert sur l'extérieur tel que celui nommé communément "internet".

La protection traditionnellement utilisée est constituée d'un logiciel habituellement appelé "fire wall".

Ce type de protection n'est pas infaillible car il ne résout pas le problème de la présence physique du réseau de communication externe sur le ou les serveur(s) de données ou de messagerie.

Le dispositif selon l'invention permet de remédier à cet inconvénient. Il comporte en effet un boîtier comprenant :

- un système d'exploitation sur technologie carte électronique à processeur avec utilitaire de configuration et de connexion au réseau extérieur de communication.
- la connexion au réseau extérieur de communication est réalisée par l'intermédiaire d'une interface "ethernet" au travers d'un réseau local avec un serveur spécialisé ou par l'intermédiaire d'un communicateur de type modem, RNIS, ADSL ou autre à titre d'exemple non limitatif.
- un système de commutation et adaptation rapide permet de "basculer" une console ou un poste de travail du réseau local et/ou externe de l'entreprise, de l'organisme ou de la structure sur le réseau extérieur de communication dit "internet" ou autre par l'intermédiaire du système d'exploitation défini ci-dessus.

Le principe consiste à ne réaliser les connexions au réseau de communication externe (internet ou autre à titre non limitatif) uniquement sur un système connexe constitué par le système d'exploitation défini ci-dessus.

Le réseau de l'entreprise, de l'organisme ou de la structure est alors complètement indépendant physiquement du réseau de communication externe (internet ou autre) ou de toute connexion vers un quelconque système de communication externe (internet ou autre. Ainsi, aucun signal et/ou aucune donnée extérieurs ne peuvent être mis en contact avec les bus adresses et données des systèmes internes (locaux ou distants) de l'entreprise, de l'organisme ou de la structure.

L'unité centrale raccordée au réseau de l'entreprise, de l'organisme ou de la structure est raccordée au présent dispositif et le clavier, la souris et l'interface d'affichage sont gérés et commutés par le système de commutation décrit ci-dessus faisant partie du présent dispositif.

Aucune connexion physique entre le réseau de communication externe ("internet" ou autre) et l'unité centrale du poste de travail n'est possible. La liaison avec le réseau externe de communication ("internet" ou autre) est réalisée par le dispositif, soit par modem soit par un autre réseau local indépendant passant par un serveur spécialisé indépendant qui n'a pas de liaison physique avec le réseau de l'entreprise, de l'organisme ou de la structure.

Dans la forme de réalisation, le système est composé :

- d'une carte électronique à et avec processeur (dite "carte mère"),
- d'une mémoire Ram de travail,
- d'une interface vidéo indépendante ou intégrée à la carte électronique sus-citée,
- d'une interface de communication interne de type ethernet ou autre pour connexion éventuelle à un serveur spécialisé,
- d'une interface de communication externe de type modem et/ou RNIS et/ou ADSL et/ou autre pour connexion éventuelle directe,
- d'une unité de stockage de masse suffisante pour recevoir le système d'exploitation, le programme interface opérateur de paramétrage, le programme de navigation sur le réseau de communication externe ("internet" ou autre), le programme de communication et messagerie, le programme de gestion des interfaces, les données de l'utilisateur,

- Une prise permettant de raccorder un lecteur de disquette et un cédérom sur le dispositif pour réglage et paramétrage,
- un système intégré de commutation de console (périphériques de dialogue homme-machine : le moniteur, le clavier et la souris),
- un système d'exploitation,
- un programme de navigation et de messagerie,
- un programme interface de configuration et de paramétrage des différents paramètres nécessaires aux modes de communication.
- une interface parallèle pour impression de documents issus du réseau externe de communication ("internet" ou autre),
- les prises pour raccorder l'unité centrale du poste de travail, le moniteur, le clavier et la souris.
- A titre d'exemple non limitatif, la connexion au réseau extérieur est réalisée dans la forme de réalisation par un logiciel de navigation et de messagerie supportés par une carte à processeur dont un port est relié à une interface réseau, RNIS, ADSL ou modem, et peut aussi être réalisée, dans des variantes, par tout système assurant la même fonction au sein du dispositif.

REVENDICATIONS

1) Dispositif pour protéger les systèmes informatiques contre les intrusions ou malveillances issues d'un réseau de communication ouvert sur l'extérieur tel que celui nommé communément "internet", étant composé :

- d'une carte électronique à processeur (dite "carte mère"),
- d'une mémoire Ram de travail,
- d'une interface vidéo indépendante ou intégrée à la carte électronique suscitée,
- d'une interface de communication interne de type Ethernet pour connexion éventuelle à un serveur spécialisé,
- d'une interface de communication externe de type modem et/ou RNIS et/ou ADSL pour connexion éventuelle directe,
- d'une unité de stockage de masse suffisante pour recevoir le système d'exploitation, le programme interface opérateur de paramétrage, le programme de navigation sur le réseau de communication externe tel que "internet", le programme de communication et messagerie, le programme de gestion des interfaces, les données de l'utilisateur,
- d'une prise permettant de raccorder un lecteur de disquette et un cédérom sur le dispositif pour réglage et paramétrage,
- d'un système intégré de commutation de console périphérique de dialogue homme-machine : tel que le moniteur, le clavier et la souris,
- d'un système d'exploitation,
- d'un programme de navigation et de messagerie,
- d'un programme interface de configuration et de paramétrage des différents paramètres nécessaires aux modes de communication.
- d'une interface parallèle pour impression de documents issus du réseau externe de communication,
- des prises pour raccorder l'unité centrale du poste de travail, le moniteur, le clavier et la souris,

fonctionnant par commutation physique de tout périphérique de dialogue opérateur avec le poste de travail, sur le système de communication externe du dispositif indépendant des réseaux de l'entreprise desservant les serveurs de données et

d'applications ; l'utilisateur disposant alors d'une console de travail tel que écran, clavier et souris, pouvant être connectée à son poste de travail qui est sur le réseau de l'entreprise ou connectée sur le dispositif qui permet l'accès à "internet" et au système de messagerie tel que serveur entreprise "web" et messagerie ou connexion directe au fournisseur d'accès.

2) Dispositif selon la revendication 1 caractérisé en ce qu'il comporte un système d'exploitation sur technologie carte électronique à processeur avec utilitaire de configuration et de connexion au réseau extérieur de communication.

3) Dispositif selon la revendication 1 caractérisé en ce qu'il comporte un système de commutation et adaptation rapide permettant de "basculer" une console ou un poste de travail du réseau local et/ou externe de l'entreprise, de l'organisme ou de la structure sur un réseau extérieur de communication tel que "internet".

4) Dispositif selon la revendication 1 caractérisé en ce que ledit dispositif de commutation ne réalise les connexions au réseau de communication externe qu'uniquement par l'intermédiaire dudit système ; et conséquemment, le réseau de l'entreprise, de l'organisme ou de la structure est complètement indépendant physiquement du réseau de communication externe, et ainsi, aucun signal ou donnée extérieurs ne peuvent être mis en contact avec les bus adresses et données des systèmes internes locaux ou distants de l'entreprise, de l'organisme ou de la structure.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 01/02466

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	STELZER G: "DER SHERIFF PASST AUF FIREWALL-ON-A-CHIP SORGT FUER DATENSICHERHEIT" ELEKTRONIK, FRANZIS VERLAG GMBH. MUNCHEN, DE, vol. 48, no. 18, 7 September 1999 (1999-09-07), page 80,82 XP000924136 ISSN: 0013-5658 abstract page 80, left-hand column, line 1 -right-hand column, line 7 --- -/--	1-4

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 December 2001	20/12/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Adkhis, F

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 01/02466

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	NEWMAN D: "SECURITY" DATA COMMUNICATIONS, MCGRAW HILL. NEW YORK, US, vol. 28, no. 1, January 1999 (1999-01), pages 44-45, XP000790858 ISSN: 0363-6399 abstract page 44, right-hand column, line 37 -page 45, left-hand column, line 19 page 45, middle column, line 27 -right-hand column, line 5	1-4
A	ELEKTRONIKNET: "Ein-Chip-Firewall: Der Sheriff kommt ins Haus" ELEKTRONIKNET TOP NEWS, 31 March 1999 (1999-03-31), XP002164257 Internet the whole document	1-4

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 01/02466

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L29/06

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	STELZER G: "DER SHERIFF PASST AUF FIREWALL-ON-A-CHIP SORGT FUER DATENSICHERHEIT" ELEKTRONIK, FRANZIS VERLAG GMBH. MUNCHEN, DE, vol. 48, no. 18, 7 septembre 1999 (1999-09-07), page 80,82 XP000924136 ISSN: 0013-5658 abrégé page 80, colonne de gauche, ligne 1 -colonne de droite, ligne 7 -/--	1-4

[X] Voir la suite du cadre C pour la fin de la liste des documents

[ ] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
14 décembre 2001	20/12/2001

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Adkhis, F

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 01/02466

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	NEWMAN D: "SECURITY" DATA COMMUNICATIONS, MCGRAW HILL. NEW YORK, US, vol. 28, no. 1, janvier 1999 (1999-01), pages 44-45, XP000790858 ISSN: 0363-6399 abrégé page 44, colonne de droite, ligne 37 -page 45, colonne de gauche, ligne 19 page 45, colonne du milieu, ligne 27 -colonne de droite, ligne 5	1-4
A	ELEKTRONIKNET: "Ein-Chip-Firewall: Der Sheriff kommt ins Haus" ELEKTRONIKNET TOP NEWS, 31 mars 1999 (1999-03-31), XP002164257 Internet le document en entier	1-4

Formulaire PCT/ISA/210 (suite de la deuxième feuille) (juillet 1992)